

Testimony of Juliette N. Kayyem

**Undersecretary for Homeland Security
Commonwealth of Massachusetts**

**“Moving Beyond the First Five Years: Evolving the Office of Intelligence and
Analysis to Better Serve State, Local, and Tribal Needs.”**

April 24, 2008

It is an honor to testify in this important matter, "Moving Beyond the First Five Years: Evolving the Office of Intelligence and Analysis to Better Serve State, Local and Tribal Needs." It is especially an honor to be here in front of Chairwoman Harman, who has not only been an exceptional leader in this field, but a friend and mentor to me as well.

I hope my testimony today will highlight some of the exceptional work performed by our Commonwealth Fusion Center, provide guidance for how this committee might think about the relationship between the states and the Department of Homeland Security (DHS) regarding intelligence efforts, and provide some thoughts on what does and does not work in the structure that now exists. And since this committee is already familiar with many of the challenges facing fusion centers, including continuing funding by homeland security grants, I will focus my discussion instead on themes and priorities. Of course, like every other homeland security advisor, I worry about sustainability and continued funding of the state's many efforts, but enough said in that regard.

The last time I testified before this committee, I was a lecturer at the Kennedy School of Government, and my focus then was on how the federal government could better collect and analyze intelligence. For the last year, I have served as the Undersecretary of Homeland Security for the Commonwealth of Massachusetts. In this position, I report to Secretary of Public Safety Kevin Burke. In addition, I am Governor Deval Patrick's federally designated homeland security advisor. In many respects, the status of my position reflects the trends and changes within homeland security on both the federal and state level. Just as Hurricane Katrina painfully taught us that a Department solely focused on terrorism may be at risk of undervaluing threats brought by mother nature, a state homeland security apparatus not aligned with the daily needs of public safety entities or first responders could not survive or remain relevant.

In this capacity, then, Governor Patrick and Secretary Burke charged me and our public safety agencies with evaluating the status of homeland security in the state to promote successful integration of our public safety and emergency management operations. Our legacy is in ensuring that policies and practices better protect our citizens from harm, wherever it may arise. So, first and foremost, this meant requiring that the state had plans and policies in place to guide the significant homeland security funds coming to the state, whether they be for interoperability, evacuation planning, resource management, recovery efforts or, as I will highlight here, intelligence efforts.

The Commonwealth Fusion Center, the CFC, is, by Executive Order, the state's designated fusion center and was established in October, 2004. The Boston Regional Intelligence Center, the BRIC, serves as the UASI's primary fusion entity, and we continue to ensure that both of their efforts are cooperative and, to the extent practicable, not duplicative. DHS needs to ensure that limited resources, capabilities and information do not unnecessarily create competition, but ensure cooperation. We have a very good working relationship with the BRIC, and the Boston police for that matter. DHS can play a very useful role in ensuring that resources are shared to create a unified system.

The CFC is, like most fusion centers, part of our state police, reporting through the chain of command to the Colonel of the Massachusetts State Police (MSP). While in the past newspaper articles and commentators have decried the fact that many fusion centers are joint tasked – intelligence and law enforcement based – I think those concerns are ill-founded. Indeed, I can't imagine a structure in which a fusion center was not, in major respects, focused on traditional crime analysis, providing information to localities and receiving important criminal trends from them in return. A fusion center that was solely terrorism focused could not sustain itself, not given the intelligence that is out there nor the competing needs of Governors and Mayors who are, as we are, concerned about crime. And because traditional crime often serves as a means for more nefarious or dangerous activities, we have to focus our efforts holistically. The true power that resides at the state and local level of law enforcement vis-à-vis terrorism prevention is not some grand new intelligence mission, but rather a culture of sharing the product of the good work that has been going on for years. The information that police officers routinely collect in the course of their normal duties is the same information that may identify terrorist financing or a pre-operational cell. It is also, it should be noted, the same information that a local chief can use to identify criminal hotspots or emerging trends.

To that end, we are working to put information and tools in the hands of state and local law enforcement that will enable them to detect and track precursor crimes as well as other trends. The Statewide Information Sharing System, or SWISS, has been funded by our homeland security dollars and while available and utile to all contributing departments, it will drastically enhance the CFC's homeland security and traditional crime missions. The dual-use concept is thoroughly ingrained in our homeland security strategy so that we might both meet head-on and mitigate the challenge of sustainability. Indeed, our fusion center is so integrated into the workings of the MSP that it is financially sustained wholly as part of the current operational costs of the MSP. While homeland security funds focus the CFC's efforts and training, we are not presently facing a wholesale crisis or the potential loss of analysts as is occurring in other fusion centers.

What is interesting here, however, is that not until recently has there been a discussion by DHS with states and localities on how the federal government could access that information in a strategic manner. A recent article in the Los Angeles Times highlights the LAPD's efforts to utilize some standardized form that would serve as a trigger for suspicious reporting to DHS. That was a local effort, and to our knowledge the most proactive attempt to treat what the fusion centers are doing as relevant to federal threat gathering. We do not need a state by state capacity to access information about specific investigations or persons; indeed, once an individual jurisdiction sends information to the FBI under Guardian, we no longer have "peeking" ability. What we need is a system in which the trends or activities that are reported to the DHS Office of Intelligence and Analysis (I&A) are done so in a systematic way, and made transparent to those who would need to know the information. Without that capability, the efforts on the state level will be of little value to DHS.

The CFC has, like most fusion centers, been an evolving entity. I sometimes imagine it like Goldilocks, searching for the "just right" fit. Ours began, like many of the post-9/11

entities, as an answer to the call from the federal government to help prevent the “next 9/11.” The changes that have occurred in the CFC, and that will continue to occur, happen because of the unique needs of our state and the changing nature of the intelligence we receive.

So, what I want to lay out here are my thoughts at this moment in time, with an eye to guiding this committee, as well as DHS, on bettering our collective efforts in the future. The CFC was one of the pilot fusion centers in the recent CENTRA report, and we learned a lot in that process. Where I critique, it is only to urge a more thoughtful assessment for the future; where I compliment, it is to provide, however anecdotally, some evidence where efforts ought to be sustained.

To begin, it might be helpful to simply lay out who is, and isn’t, at the fusion center now and what they do. The core of the CFC is staffed with MSP personnel, who first and foremost are responsible to their chain of command. Representatives from other agencies include one Federal Bureau of Investigation (FBI) analyst, one agent and one analyst from the Bureau of Alcohol, Tobacco, Firearms and Explosives, one counter-drug analyst from the Massachusetts National Guard, one analyst from the Department of Correction (currently deployed to Iraq), one representative from DHS I&A, one police officer from CSX railroad, and a Geographic Information Systems specialist from the U.S. Army Civil Support Team. In addition, several MSP troopers under the direct command of the CFC, and therefore the Executive Office of Public Safety and Security, are assigned to the FBI Joint Terrorism Task Force (JTTF) for specific investigation support.

The primary focus for today’s hearing is on the Office of Intelligence and Analysis, and how it works with state fusion centers. We are fortunate to be a state with a designated I&A analyst. She had previously worked at the fusion center, and so her knowledge of it, and the state itself, has been a tremendous asset.

She is, for the fusion center, and for me specifically, our one stop shopping. While she may not have every answer at hand, she knows how to get it for us. We should not underestimate how important that is. DHS, for any state, can be both amorphous and large. In Massachusetts alone, the DHS entities – from ICE, to Coast Guard, to FEMA, to a critical infrastructure analyst, to chemical industry regulators, to TSA – are all professional, but from the perspective of a state, are also too numerous to count. While FEMA has taken the lead on trying to integrate these entities, the truth is that their mission and chains of command so vary that it can be difficult. For us to have one liaison that can tap into, at the very least, intelligence efforts at DHS, and across the federal government, has proven exceptionally helpful. There are, after all, 16 federal agencies that make up the Intelligence Community, all attempting to assess the persistent and evolving threats this nation faces. It may be, one wonders, too many for the federal government; it is certainly too many for a single state. As one of our fusion center analysts noted, our I&A analyst provides a mechanism to reach into the “quagmire” and get the information and resources needed by the state.

This is particularly true in one aspect of our needs: Requests for Information (RFI). Working with the CFC and the BRIC, and due to the CENTRA assessments, I&A submitted recommendations for creating a process which would efficiently serve the state's needs. This process was concluded before the CENTRA report findings, but is supported by that report. While I cannot disclose the details of the requests we have made, they have revolved around unique aspects and threats to our state and to Boston, whether they be related to critical infrastructure or visits by foreign dignitaries. I&A provides connectivity and rapid response for us; some requests are returned with information within hours of being relayed. This information can then be utilized to guide operational planning by the state police or local law enforcement.

There are other benefits, including access to secure cell phones for state designees and getting through the red tape that often is involved in security clearances. Indeed, in a recent trip I took to Paraguay, a nation that has a relationship with the state's National Guard, our I&A analyst was able to successfully transition our security clearances to the state department with one day's notice.

Thus, the physical presence of a single person who can tap into DHS, who knows why we are asking and what it means for the state, has gone exceptionally far in our relationship with DHS regarding intelligence efforts.

However, it is in the CFC's role as a consumer of intelligence that many of the more persistent difficulties arise. First, the CENTRA report, which I have studied, places tremendous emphasis on making intelligence more accessible to states and localities. That is an important effort. But, while DHS focuses these efforts on ensuring that the quantity of information getting to us continues to flow, we are likely similar to many other states in wondering whether we aren't at risk of threat assessment fatigue.

Let me put this another way. We have placed so much focus on ensuring that intelligence flows horizontally and vertically from and to state and federal governments that we may be at risk of the intelligence version of the often quoted academic trajectory: publish or perish. The quantity of information coming to us, often without much reference to either its strategic or tactical relevance, is overwhelming. And, as a state, we are left in a bit of a dilemma: distribute the information and risk triggering responses that are not justified by the validity of the intelligence or simply close-hold the information and be at risk of recreating the very stovepipes this whole effort was meant to destroy. Thus, while DHS assesses its own intelligence capabilities in the years to come, and under a new president from either party, the quality of the intelligence being shared has got to be an essential aspect of that conversation.

A relatively public example may be helpful. In 2008, there have been a number of Osama bin Laden audiotapes. We received notification of each of them by DHS (as well as by the FBI) but also, I must admit, by CNN. Their substance, for those of us who follow these things, was nothing novel: the literal rantings of the terrorist against everything associated or affiliated with the United States. But, as we all know, we need to remain exceptionally vigilant during times of democratic transition; both Spain and the

United Kingdom were victims of terrorist attacks immediately before or immediately after a change in government. So while the fact of the tapes didn't seem to raise anything new in our mind, and the literal statements didn't seem particularly worrisome, as more and more audiotapes came out (and may continue to be released), we would want to be in a position to know how the federal government is assessing this, how are they thinking through this summer and fall of transition, and whether we shouldn't be doing the same. It is that kind of strategic guidance that would be helpful.

I am relatively confident that any information that is worthy of a preliminary or criminal investigation will be properly vetted and analyzed by our JTTF, where many of our CFC troopers work. But, for the majority of information, call it white noise or background atmospherics, we are simply consumers, not quite able to decipher whether there is any strategic relevance to so much information, but pretty confident that our operational assessments will not change.

Second, and this is not something we can fix on the state level, DHS needs to ensure that the kinds of guidance we are receiving from other DHS entities or other federal entities is aligned with the very intelligence we are receiving from I&A. Most recently, the states received guidance and priorities for the major state homeland security grant cycle, which concludes in May. This is the major grant that states and the UASIs receive to support first responder capabilities. While we know that IEDs continue to be a threat in Iraq and against our soldiers abroad, no intelligence we had received from DHS or any federal entity prepared us for the explicit focus that the grant now has on IED prevention, protection, and response planning. To be clear, this is an important effort, one that needs attention and one that we have and will continue to address, in particular with our critical infrastructure program, which I will discuss further in a moment. But, by explicitly focusing on IEDs, we were left wondering whether we proverbially didn't know what we didn't know. Or, for another example, the Buffer Zone Protection grants are annually distributed to critical infrastructure sites to buttress prevention and law enforcement efforts. At the same time, some specific industries – say telecommunications or water purifying sites – will be chosen for site visits. From what we know, on the state level, these industries are chosen without us knowing why, and certainly without the industry knowing why. It may be, as I believe now, that DHS is doing due diligence and ensuring that states focus on many different sectors. But, since there is no intelligence to decipher why a specific industry is chosen, or in one case in our state, a specific site, we are left explaining to our private sector partners to simply accept the designation, trying to assure them that they are not at increased risk.

This gets me to the final comment on the challenges of our “consumer” role. Intelligence can be inherently vague and hard to define; with it, comes a tremendous amount of responsibility. While we continue to live with threats, from terrorists or bad actors or even from mother nature, the knowledge of those threats demands that those of us who work and respond to them act professionally and in a reasoned fashion. When intelligence goes from atmospherics, to potentially a real threat, we need to ensure that the very processes we have put into place are utilized and reinforced. This was made entirely clear from our recent responses to the potential consequences of an NRO spy

satellite falling to earth. From my perspective, I don't really care if the Secretary of Defense, the Secretary of Homeland Security or even the Secretary of Agriculture, if he is so inclined, is designated the principal federal officer for an event. The concern is that, as the other homeland security advisors shared information they were receiving in that two week period leading up to the successful Defense Department downing of the satellite, it was clear that we simply didn't have a unified notion of how we ought to prepare our public safety agencies, let alone the public. There was also a lack of a reality check in all the chaos that could answer whether the real issue at hand was one of a danger to the public for emergency management planning purposes, or a danger to our national security in that secret information might be disclosed if pieces of the satellite fell in adversary hands. It was in that vacuum that, I believe, each state likely planned differently, based on information that we all believed was probably not forthcoming. Perhaps it was because there was confidence that the Defense Department would successfully shoot down the satellite, or perhaps because the trajectory couldn't actually be determined, or maybe we knew less because the trajectory never made its way to New England, but it was in that vacuum that both paranoia and gossip gets started, and when confidence in the entire process gets undermined. The states must be treated as mature partners in these intelligence efforts.

As we look forward as well, I want to add two important efforts into the mix of how we should be thinking of DHS and I&A intelligence functions in the future. We need to continue, as we do in all homeland security efforts, to provide policies and practices that will be dual-use and respond to many hazards. Thus, as we think about the legacy of fusion centers and their continuing viability, one of the major arenas where they will and can provide unique value is in critical infrastructure assessments. In the past, our state's critical infrastructure assessments were locally based, providing the state with hundreds of potential and vulnerable sites, ranging from nuclear facilities to local high schools. Both are, of course, important, but we had no mechanism to focus these efforts on risk reduction and, from the perspective of the state, response needs.

Specific intelligence against a particular site, and our response to that information, is different than the kind of analysis we are now supporting through the fusion center in Massachusetts. Indeed, many of the homeland security dollars going to the CFC are now supporting training and efforts related to creating a unified critical infrastructure assessment tool, known as ACAMS, which is supported by DHS. We know, and explicitly express in the Commonwealth's State Homeland Security Strategy^[1], that in order to effectively carry out their missions, public safety officials and policy makers need a comprehensive understanding of the vulnerabilities of assets, systems, networks, and functions that provide critical services to the people of the Commonwealth. This knowledge will drive public safety and public policy decisions regarding preventative and protective measures, as well as response activities to natural and man-made incidents. We are committed to understanding and assessing risk in the Commonwealth by ranking what assets are in the state based upon their vulnerabilities, whether they are likely to be

[1]

<http://www.mass.gov/?pageID=eopssubtopic&L=3&L0=Home&L1=Homeland+Security+%26+Emergency+Response&L2=State+Homeland+Security+Strategy&sid=Eeops>

under threat, and how their destruction, through any means, would impact the state. ACAMS and the CFC provide a statewide, coordinated approach to the identification, prioritization, and protection of critical infrastructure and key resources that can be shared with important stakeholders and emergency response personnel. For this to be a successful effort, we must also partner with I&A to ensure that their strategic knowledge is shared and disseminated.

Another such critical infrastructure initiative that has recently begun to take shape at the CFC in regard to critical infrastructure is a relationship between the CFC and the Nuclear Regulatory Commission (NRC). At the recent fusion center conference in San Francisco, it was brought to our attention that there exists an NRC database cataloging suspicious activities reported by utility companies throughout the country. Being a state with one active nuclear power plant and two others in bordering states that affect Massachusetts' communities within the 10 mile emergency planning zone, we were intrigued by this information and the opportunity to further our critical infrastructure protection efforts utilizing the NRC database. We have reached out to the NRC and are beginning a process in which the NRC, the CFC, and our emergency management agency will communicate on issues of suspicious activity involving radiological threats.

I believe that these efforts, in conjunction with DHS and I&A, are really the foundation of a legacy for fusion centers nationwide. Not simply because we can better prevent and respond to terrorist threats against our critical infrastructure, but also because we can know, beforehand, how we might prioritize any number of important public safety and public policy needs.

Finally, and this is something that I know Chairwoman Harman promotes, we need to continue to demand that fusion centers are as transparent as possible, ensuring that they serve our important public safety needs in a democratic society. There will always be a tension between liberty and security, but the tension need not impede honest discussion and even evaluation. I believe, as someone who began her career in the Justice Department's Civil Rights Division, and someone who has written extensively in this regard, that we may never permanently settle this issue, but we must always be prepared to have the discussion. Before I came to work for the Commonwealth, my notion of what was going on in the intelligence world was not always a benign one.

The balance at the CFC and in the state we are trying to achieve now has made us reexamine our efforts, our policies, and our transparency. In response to the most recent ACLU examination of fusion centers, we vowed to provide a reply with an honest assessment of where we were and where we hoped to be in the future. That letter is attached for your review. We are, in addition, promoting a privacy council to ensure that we have the benefit of outside council not on specific investigations, but on how the state's public safety agencies might better balance their important public safety mission with the rights of our citizens. I am confident that we are closer now, but I am also confident that the world is changing so quickly and access to information, databases, and technology is so rapidly evolving, that we can not simply rest on such assurances. Such advice need not just apply to the fusion centers, but perhaps to any entity that utilizes

intelligence and information sharing as a prevention, protection, and mitigation tool. As information becomes more readily available, and the risks (as well as the benefits) are more easily multiplied, we must formalize structures and policies that embrace the debate, rather than deny or ignore it. We are not alone in our state, and to the extent that DHS can serve as a model or provide the very practices we all are seeking to achieve, we will ensure that we will take the proper steps to protect privacy and civil liberties, while continuing to utilize the mechanisms of intelligence and analysis that help protect our citizens from critical incidents.

I hope I have provided you with useful information to assess and enhance DHS I&A. I have discussed the issues that are at the forefront of the CFC's concerns; which we know also hit home with many other fusion centers. Efforts on the part of DHS and the federal government to address the issues that were raised today offer a solid basis for making improvements and continuing useful efforts by I&A.